0790326
Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 11

5th – 7th May 2024

جامعة فيلادلفيا
Philadelphia University

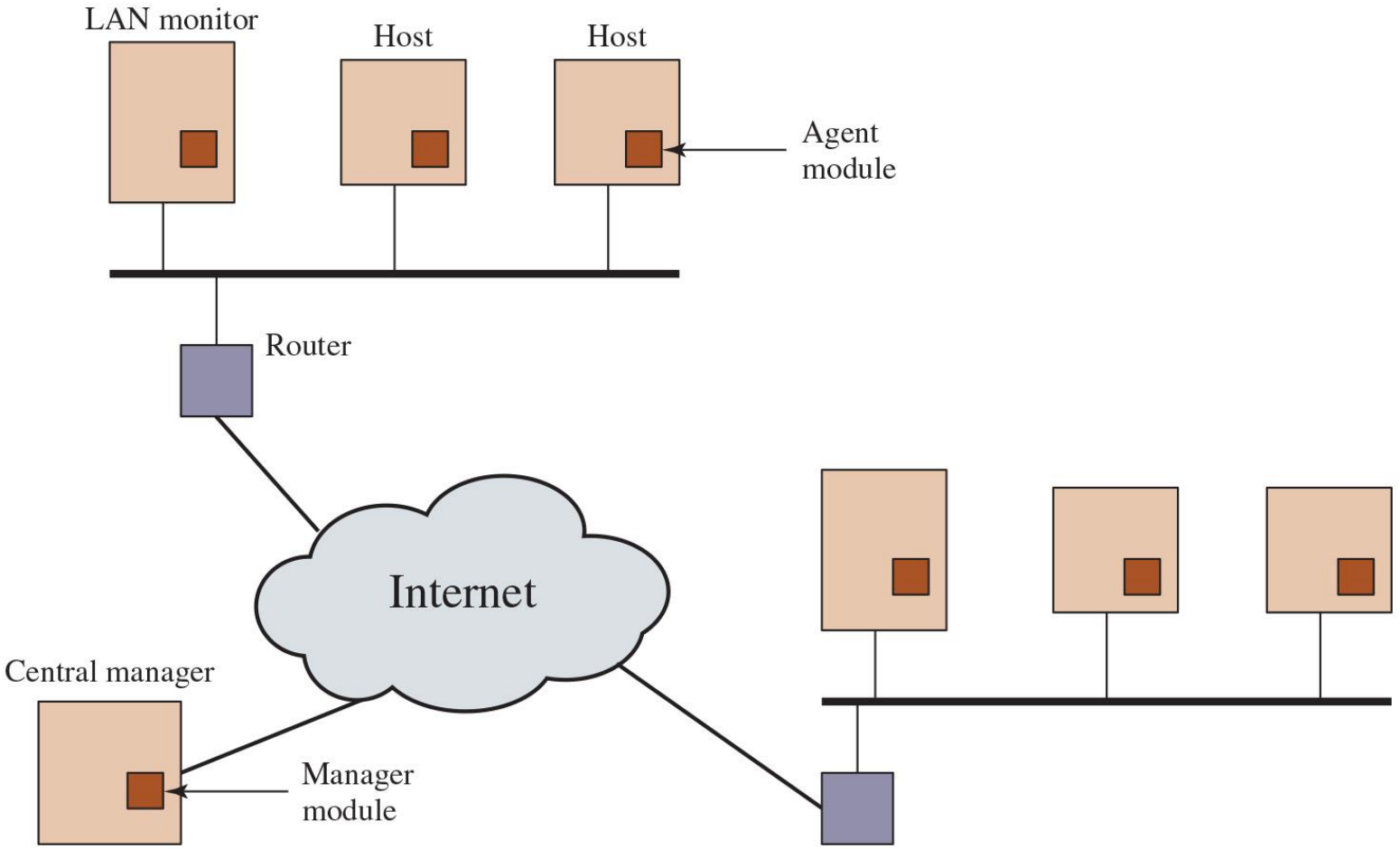
Dr. Basil Elmasri
balmasri@philadelphia.edu.jo

External Material

- Rest of the slides for this week are based on (Stallings & Brown, 2024) book, chapter 8.
  - Some extra slides have been added, their text was taken from the book.
  - Footers, dates, and slides number have been added only to help students reading the material.
- Study and exams will be based on the book chapters, not the slides.

Figure 8.2

Architecture for Distributed Intrusion Detection



Architecture for Distributed Intrusion Detection (I)

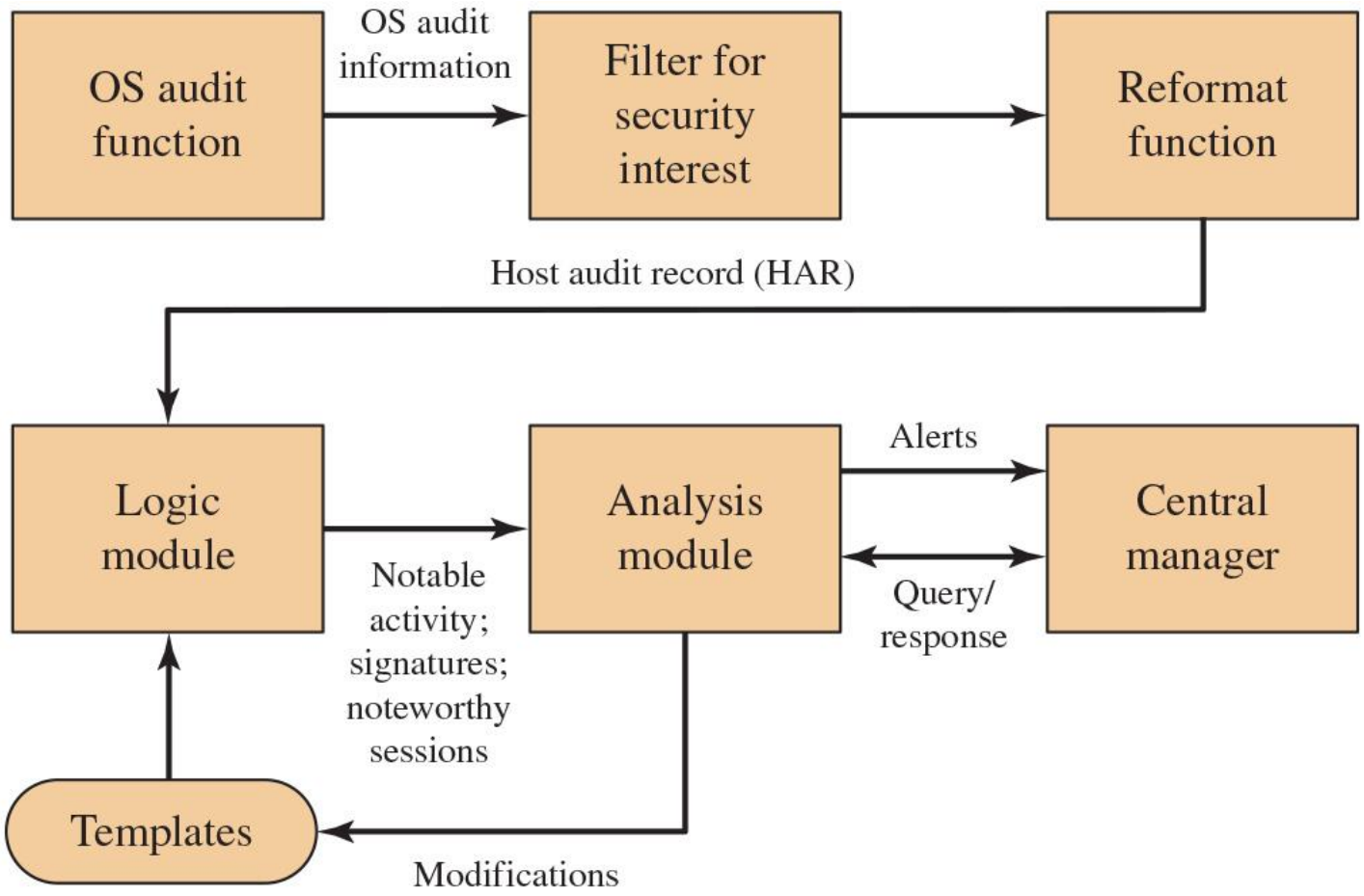
- **Host agent module**: An audit collection module operating as a background
- process on a monitored system. Its purpose is to collect data on security related events on the host and transmit these to the central manager. Figure

Architecture for Distributed Intrusion Detection (II)

- **LAN monitor agent module**: Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager.
- **Central manager module**: Receives reports from the LAN monitor and host agents and processes and correlates these reports to detect intrusion.

Figure 8.3

Agent Architecture

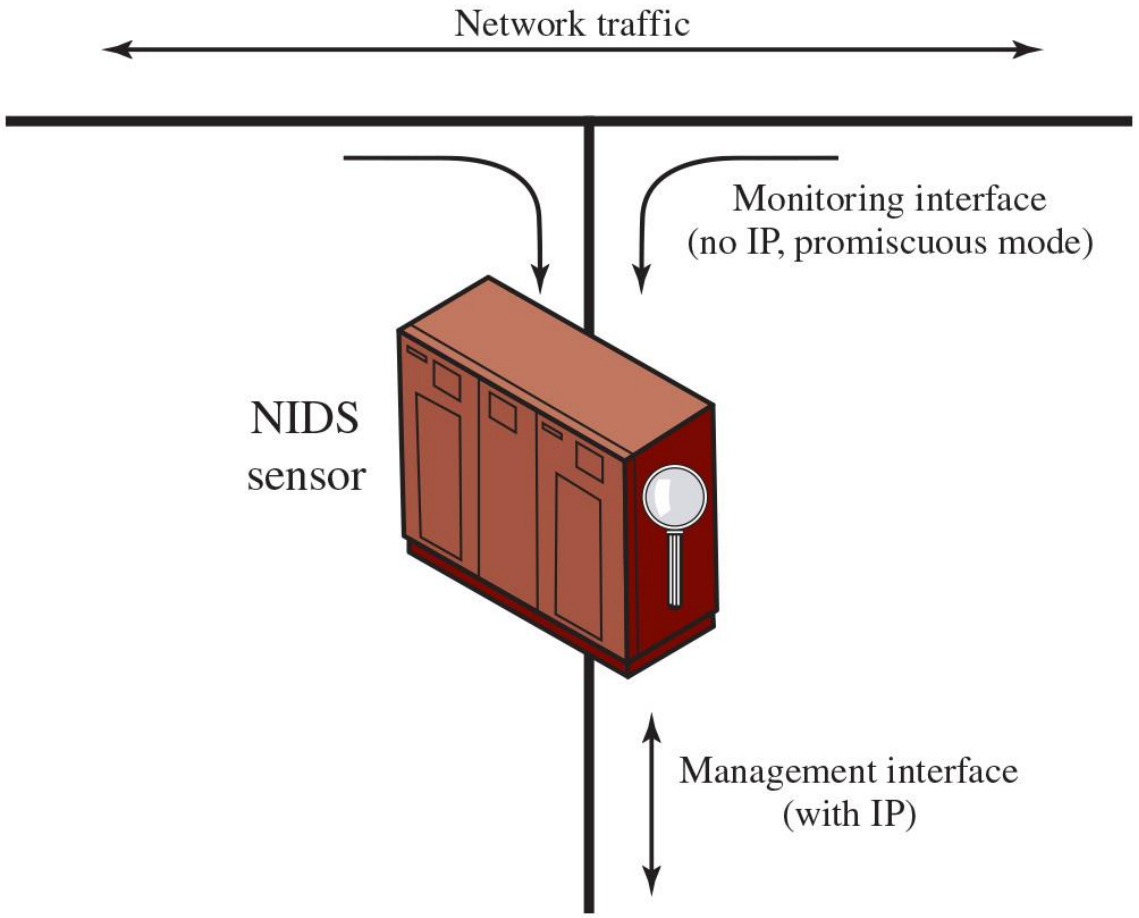


Network-Based IDS (NIDS)

- Monitors traffic at selected points on a network
- Examines traffic packet by packet in real or close to real time
- May examine network-, transport-, and/or application-level protocol activity
- Includes a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface
- Analysis of traffic patterns may be done at the sensor, the management server or at a combination of the two

Figure 8.4

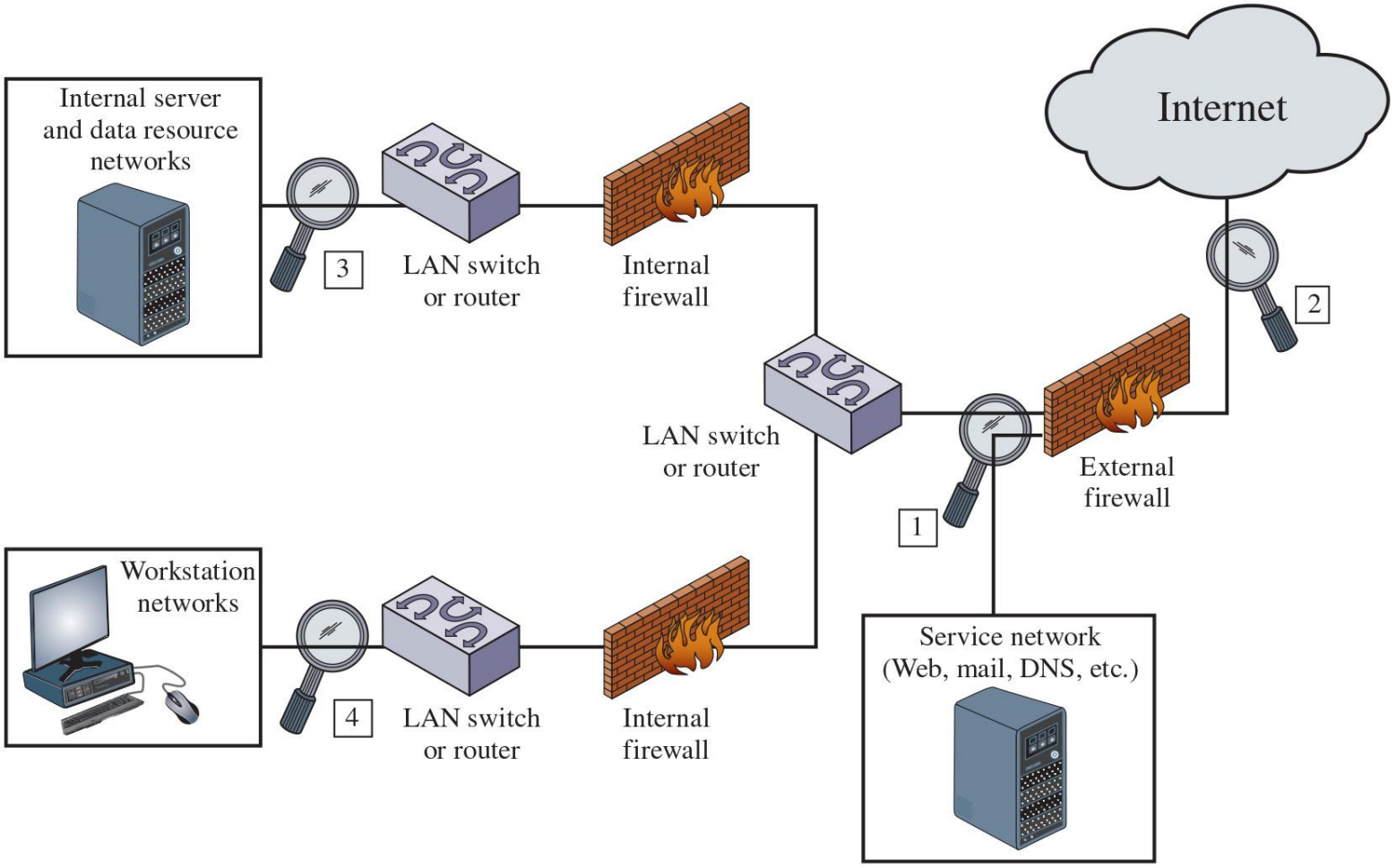
Passive NIDS Sensor



Source: Based on [CREM06].

Figure 8.5

Example of NIDS Sensor Deployment



Intrusion Detection Techniques

Attacks suitable for Signature detection

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations

Attacks suitable for Anomaly detection

- Denial-of-service (DoS) attacks
- Scanning
- Worms

Stateful Protocol Analysis (SPA)

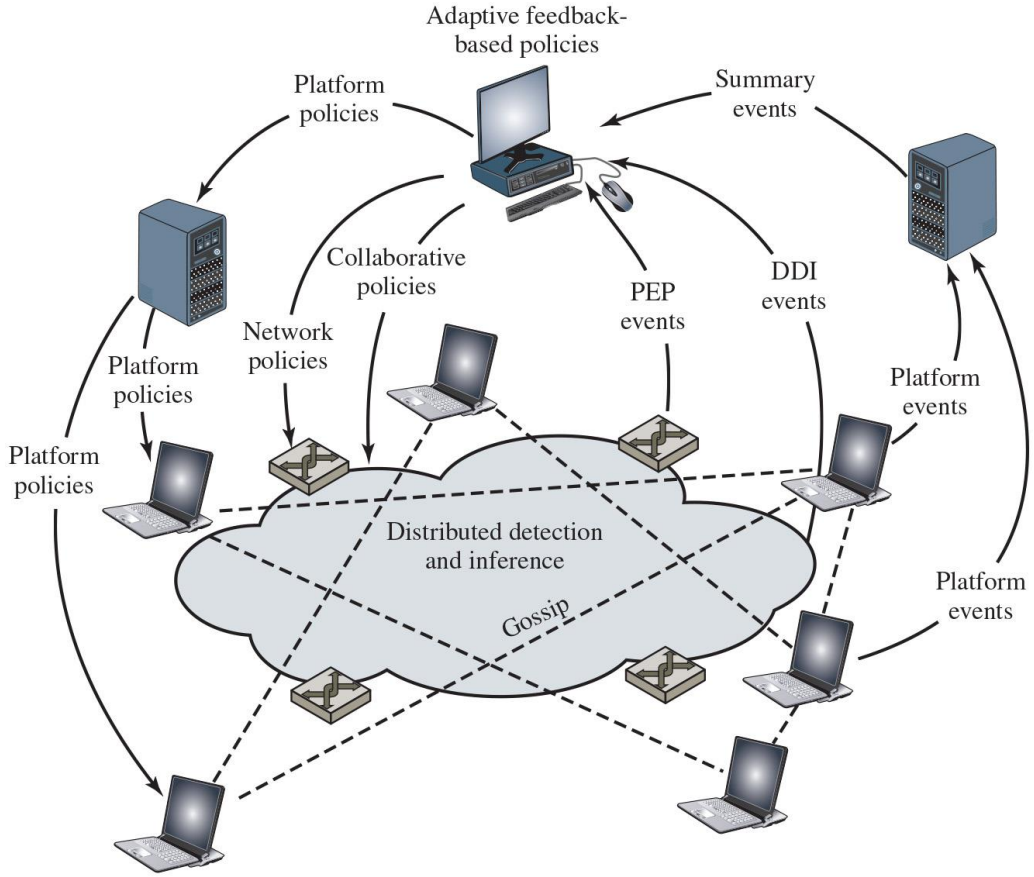
- Subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic
  - This distinguishes it from anomaly techniques trained with organization-specific traffic protocols
- Understands and tracks network, transport, and application protocol states to ensure that they progress as expected
- A key disadvantage is the high resource use it requires

Logging of Alerts

- Typical information logged by a NIDS sensor includes:
  - Timestamp
  - Connection or session ID
  - Event or alert type
  - Rating
  - Network, transport, and application layer protocols
  - Source and destination IP addresses
  - Source and destination TCP or UDP ports, or ICMP types and codes
  - Number of bytes transmitted over the connection
  - Decoded payload data, such as application requests and responses
  - State-related information

Figure 8.6

Overall Architecture of an Autonomic Enterprise Security System



PEP = policy enforcement point
DDI = distributed detection and inference

IETF Intrusion Detection Working Group (1 of 3)

- Purpose is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to management systems that may need to interact with them
- The working group issued the following RFCs in 2007:

IETF Intrusion Detection Working Group (2 of 3)

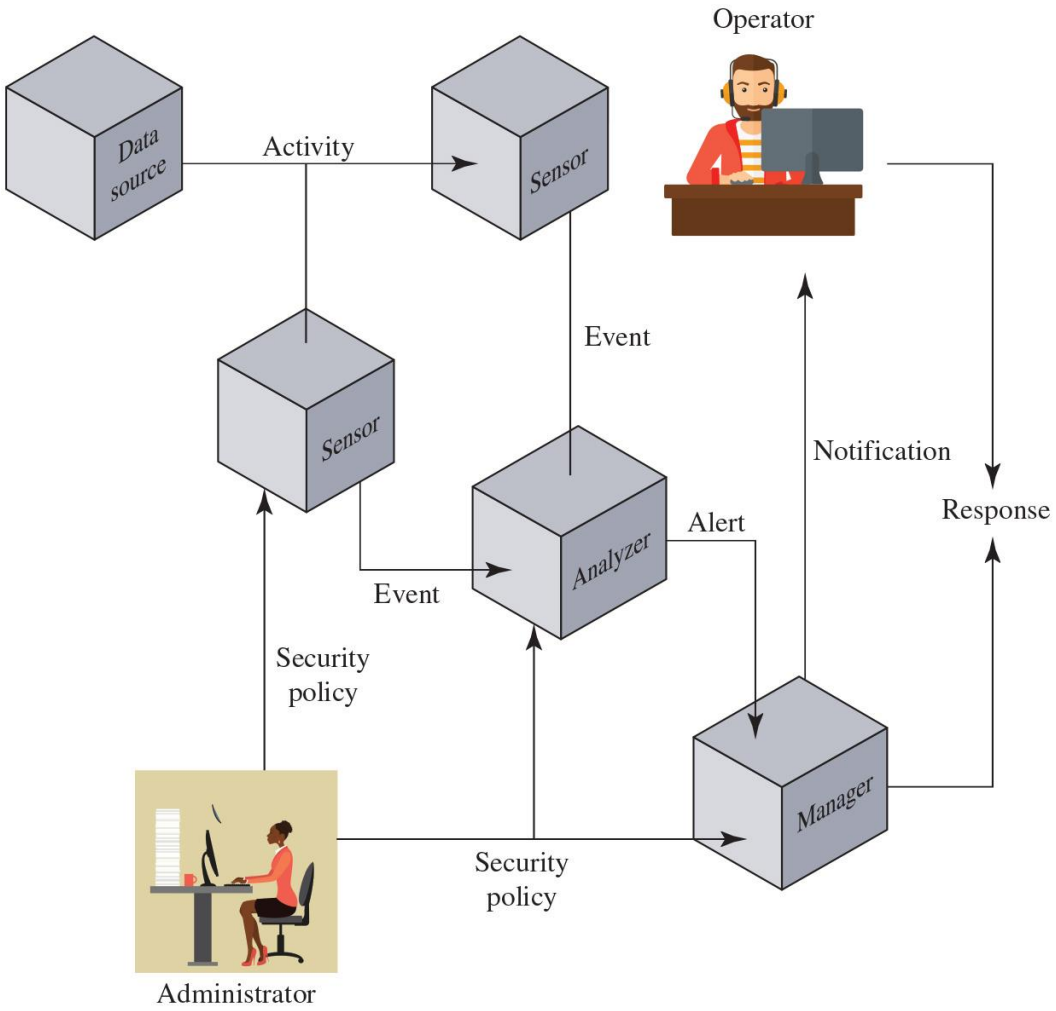
- Intrusion Detection Message Exchange Requirements (RFC 4766)
  - Document defines requirements for the Intrusion Detection Message Exchange Format (IDMEF)
  - Also specifies requirements for a communication protocol for communicating IDMEF
- The Intrusion Detection Message Exchange Format (RFC 4765)
  - Document describes a data model to represent information exported by intrusion detection systems and explains the rationale for using this model
  - An implementation of the data model in the Extensible Markup Language (XML) is presented, and XML Document Type Definition is developed, and examples are provided

IETF Intrusion Detection Working Group (3 of 3)

- The Intrusion Detection Exchange Protocol (RFC 4767)
  - Document describes the Intrusion Detection Exchange Protocol (IDXP), an application level protocol for exchanging data between intrusion detection entities
  - IDXP supports mutual authentication, integrity, and confidentiality over a connection oriented protocol

Figure 8.7

Model for Intrusion Detection Message Exchange



Honeypots

- Decoy systems designed to:
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- Systems are filled with fabricated information that a legitimate user of the system wouldn't access
- Resources that have no production value
  - Therefore incoming communication is most likely a probe, scan, or attack
  - Initiated outbound communication suggests that the system has probably been compromised

Honeypot Classifications (1 of 2)

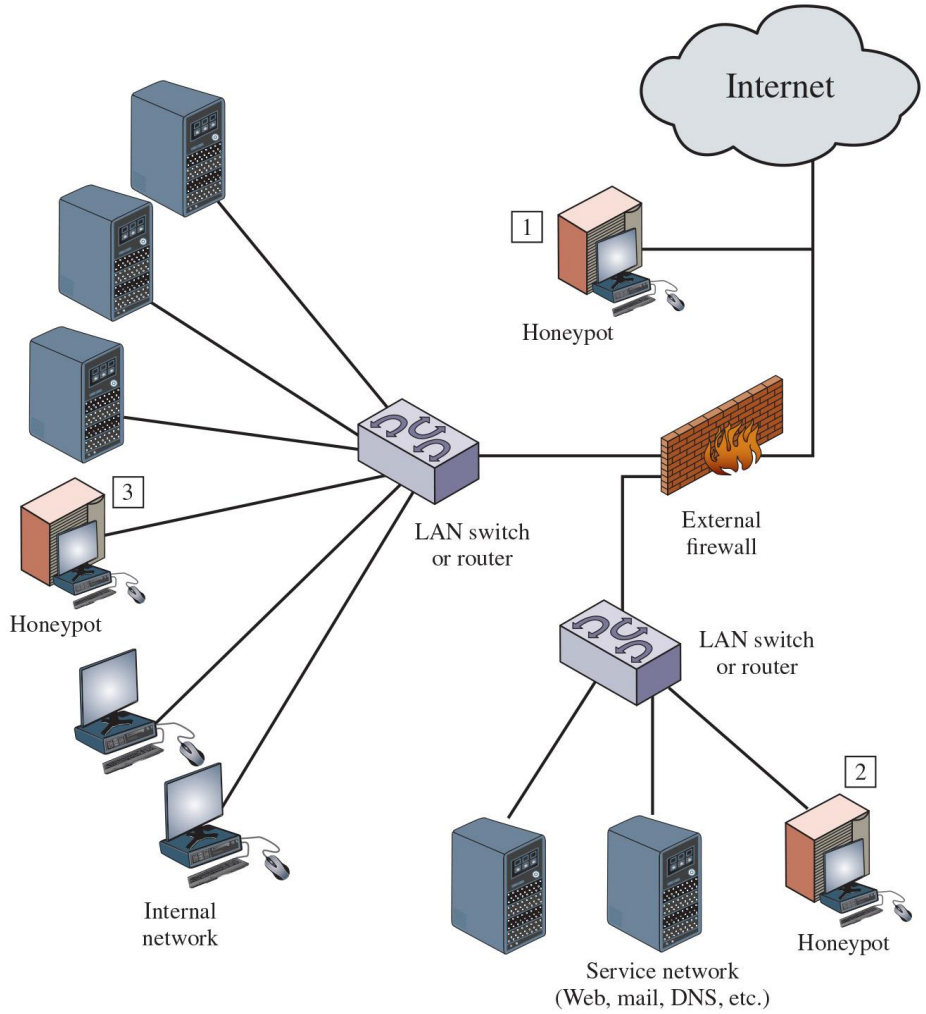
- Low-interaction honeypot
  - Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
  - Provides a less realistic target
  - Often sufficient for use as a component of a distributed IDS to warn of imminent attack

Honeypot Classifications (2 of 2)

- High interaction honeypot
  - A real system, with a full operating system, services, and applications that are instrumented and deployed where they can be accessed by attackers
  - Is a more realistic target that may occupy an attacker for an extended period
  - However, it requires significantly more resources
  - If compromised could be used to initiate attacks on other systems

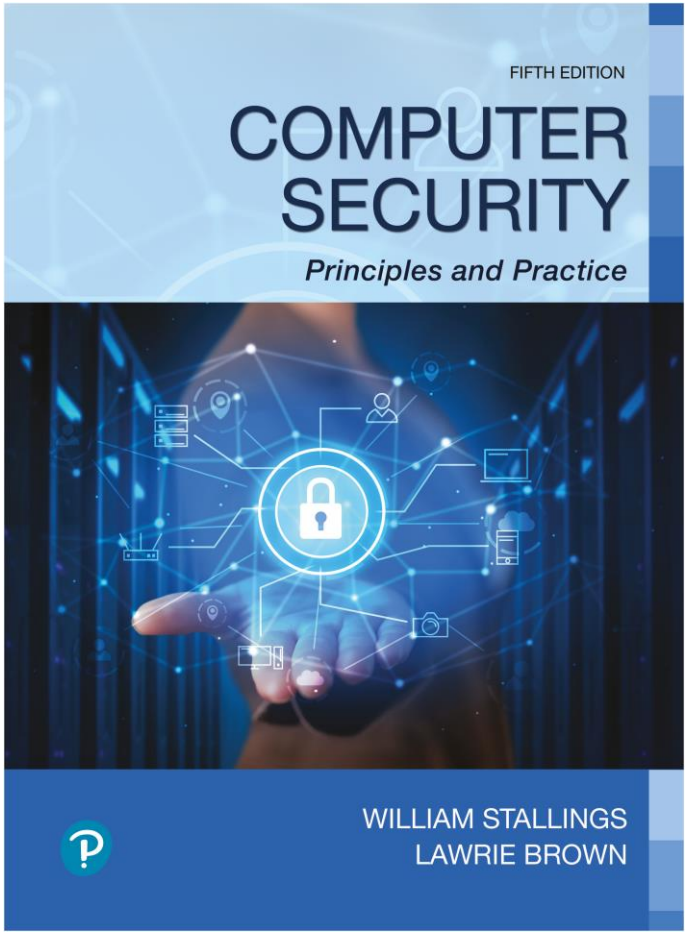
Figure 8.8

Example of Honeypot Deployment



Computer Security: Principles and Practice

Fifth Edition



Chapter 9

Firewalls and Intrusion Prevention Systems

References

Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice (5 ed.). Pearson. Retrieved from https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000010333/9780138091712